UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,769	10/11/2001	Michael C. Dapp	FS-00510 (02890038AA)	7586

181	7590	04/26/2006

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER
HENEGHAN, MATTHEW E

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>27 February 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-20 and 22-48</u> is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) <u>29 and 35-48</u> is/are allowed.

6)☒ Claim(s) <u>1-20, 22-28 and 30-34</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>22 September 2005</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All   b)☐ Some * c)☐ None of:

       1.☐ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>2/27/06, 3/23/06</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   In response to the previous office action, claims 1, 11, 20, 25, 26, 29, 35, and 44 have been amended and claim 21 has been cancelled. Claims 1-20 and 22-48 have been examined.

Information Disclosure Statement

2.   The information disclosure statements (IDS) submitted on 27 February 2006 and 23 March 2006 was filed after the mailing date of the most recent non-final rejection on 13 December 2005. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

3.   The tenth and eighteenth items on Sheet 1 and the fourth item on Sheet 2 of the IDS filed 27 February 2006 cited invalid patent publication numbers and were not considered.

4.   The seventh item on Sheet 5 of the IDS filed 27 February 2006 was not found in the file wrapper and not considered.

Claim Objections

5.   In view of Applicant's amendments, all previous claim objections are withdrawn.

Claim Rejections - 35 USC § 112

6.   In view of Applicant's amendments, all previous rejections under 35 U.S.C. 112

are withdrawn.

Claim Rejections - 35 USC § 103

        The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 1, 2, 4, 8, and 9 are rejected under 35 U.S.C. 103(a) as being

unpatentable over U.S. Patent No. 5,606,668 to Shwed in view of U.S. Patent No.

6,233,704 to Scott et al.

        As per claims 1 and 9, Shwed discloses a computer (the engine) have a packet

filter module (the data processor). Traffic is diverted to the packet filter, which tests the

packet against the packet filter's rules (i.e. rules that are used to determine abnormal

usage). If a rule is matched, an alert may be issued, which is sent to the computer for

forwarding to the user. This is all user transparent (see column 7, lines 14-47). This system is used on a router (see column 3, lines 44-48). The monitoring of alerts is performed at the system administrator's workstation (see column 4, lines 27-42), which is a different node from the router (see figure 1).

Shwed does not discuss the remediation of node faults through the selection of redundant communication paths.

Scott discloses a system wherein remedial action by network management is triggered by a node fault. The membrane topology functions in a manner corresponding to a firewall. Scott further shows redundant connections to network nodes, as a ring and counter-ring; the severing of these rings in response to a node fault causes the communications system to select paths to the respective nodes based upon the remaining non-severed paths (see column 4, line 29 to column 5, line 58). Scott further suggests that as long as faulty nodes are kept on a network, they can cause damage (see column 1, lines 47-50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shwed by taking remedial action by network management in the event of a node fault using redundant connections, as disclosed by Scott, since as long as faulty nodes are kept on a network, they can cause damage.

As per claim 2, such systems inherently use memory buffers for the communications.

Regarding claim 4, the functionality is inherently performed in real-time.

Regarding claim 8, the rules are disclosed as being "security rules." Such rules are implemented to counter potential attacks.

8.   Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed in view of U.S. Patent No. 6,233,704 to Scott et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,119,236 to Shipley et al.

Shwed and Scott do not disclose the isolation of a network node.

Shipley, which is disclosed as being an improvement over Shwed, discloses the blocking all access to the LAN from a sender which is associated with a security breach (see column 8, lines 4-9 and column 10, lines 25-27), and further notes that prior art firewalls are subject to breach by any new and unique methods of circumventing security (see column 2, lines 56-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Shwed and Scott by blocking all access to the LAN from a sender which is associated with a security breach, as disclosed by Shipley, as prior art firewalls are subject to breach by any new and unique methods of circumventing security.

9.   Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed in view of U.S. Patent No. 6,233,704 to Scott et al. as

applied to claim 1 above and further in view of U.S. Patent No. 5,737,526 to Periasamy et al.

Shwed and Scott do not discuss the hierarchical relationships among different nodes.

Periasamy discloses a hierarchically-arranged network arrangement wherein different nodes can be freely arranged among peer networks. Periasamy further discloses that this reduces broadcast traffic on slow links (see column 2, lines 49-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shwed and Scott by using a hierarchically-arranged network arrangement, as disclosed by Periasamy, to reduce broadcast traffic on slow links.

10.   Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed in view of U.S. Patent No. 6,233,704 to Scott et al. as applied to claim 1 above and further in view of Kent, RFC 2401, "Security Architecture for the Internet Protocol," 1998.

Shwed and Scott do not discuss session construction within a network.

Kent discloses the construction of secure sessions in IP networks, and specifies packet information having the identification of a communicating node (see examples on p. 16), and further suggests that this allows for the enforcement of a security policy in an IP environment (see p.14).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shwed and Scott by supporting

secure packet information having the identification of a communicating node, as

disclosed by Kent, as this allows for the enforcement of a security policy in an IP

environment.

11.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 5,606,668 to Shwed in view of U.S. Patent No. 6,233,704 to Scott et al. as

applied to claim 1 above and further in view of U.S. Patent No. 6,301,668 to Gleichauf

et al.

Shwed and Scott do not discuss the management of the various nodes.

Gleichauf discloses a system for maintaining a network map having real-time

information for all nodes in a network for assessing network vulnerabilities (see column

7, lines 26-60), and further notes that can more reliably detect policy violations and

patterns of misuse (see column 3, lines 7-13).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shwed and Scott by maintaining a

network map, as disclosed by Gleichauf, in order to more reliably detect policy violations

and patterns of misuse.

12.   Claims 11-13, 15, 17, 25-28, 30, and 32 are rejected under 35 U.S.C. 103(a) as

being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. as applied to claim

20 above, and further in view of U.S. Patent No. 5,922,049 to Radia et al.

Regarding claims 11 and 17, Shipley discloses a system for wherein several

methods are disclosed for detecting abnormal usage characteristics (see column 5, line

58 to column 6, line 67). The system user-transparently then reacts by blocking all

access to the LAN from a sender which is associated with a security breach (see

column 8, lines 4-9 and column 10, lines 25-27). A signal is transmitted from the INSD

(the first node) to the firewall via a serial connection or LAN connection; they therefore

constitute separate nodes. The detecting step is performed at the INSD, while the

corrective steps are performed at other corresponding nodes, such as the firewall (see

column 5, lines 1-43).

The invention of Shipley disallows network access to users attempting a security

breach, i.e. a potential attack (see column 8, lines 8-17); this can only be done at the

point where the user enters the network (such as the router 22 in Figure 1). Shipley's

exemplary configuration also only includes a single router, and describes this as a

"simplified" configuration, and notes that the configuration may include "other such

devices" (see column 5, lines 25-31); Shipley therefore suggests that the configuration

may contain multiple routers.

Shipley does not disclose the use of locking in routers.

Radia discloses that the use of IP address locking, in order to prevent systems from forging IP addresses to fool the router into incorrectly relearning routes (see column 3, lines 5-13).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Shipley by using locking in routers, as disclosed by Radia, in order to prevent systems from forging IP addresses to fool the router into incorrectly relearning routes.

As per claim 12, Shipley discloses the use of RAM for program execution (see column 4, line 45).

Regarding claim 13, all such processing is performed in real-time.

Regarding claim 15, all modern network implementations having at least the number of nodes as depicted in Figure 1 of Shipley are inherently capable of supporting at least two sessions (secure or otherwise) between at least two pairs of nodes.

Regarding claims 25 and 32, nodes in the same network (including the routers and firewall) are communicatively connected. Multiple nodes (i.e. the first and second nodes) can be managed.

Regarding claim 26, Shipley discloses a LAN (Local Area Network) port and a serial port (which is also a type of network port) connected to (and therefore controlled by) the INSD.

Regarding claims 27 and 28, only the nodes that need to be controlled are controlled.

Regarding claim 30, as it is unclear what the first node actually is (see Rejection under 35 U.S.C. 112, above), this claim is being considered to stand or fall with its base claim.

13.   Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claim 11 above and further in view of U.S. Patent No. 5,737,526 to Periasamy et al.

Shipley and Radia do not discuss the hierarchical relationships among different nodes.

Periasamy discloses a hierarchically-arranged network arrangement wherein different nodes can be freely arranged among peer networks. Periasamy further discloses that this reduces broadcast traffic on slow links (see column 2, lines 49-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by using a hierarchically-arranged network arrangement, as disclosed by Periasamy, to reduce broadcast traffic on slow links.

14.   Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claim 15 above and further in view of Kent, RFC 2401, "Security Architecture for the Internet Protocol," 1998.

Shipley and Radia do not discuss session construction within a network.

Kent discloses the construction of secure sessions in IP networks, and specifies

packet information having the identification of a communicating node (see examples on

p. 16), and further suggests that this allows for the enforcement of a security policy in an

IP environment (see p.14).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shipley and Radia by supporting

secure packet information having the identification of a communicating node, as

disclosed by Kent, as this allows for the enforcement of a security policy in an IP

environment.

15.   Claims 18 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to

Radia et al. as applied to claims 11 and 25 above and further in view of U.S. Patent No.

6,233,704 to Scott et al.

Shipley and Radia do not discuss the remediation of node faults.

Scott discloses a system wherein remedial action by network management is

triggered by a node fault. The membrane topology functions in a manner corresponding

to a firewall (see column 4, line 29 to column 5, line 58). Scott further suggests that as

long as faulty nodes are kept on a network, they can cause damage (see column 1,

lines 47-50).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shipley and Radia by taking

remedial action by network management in the event of a node fault, as disclosed by

Scott, since as long as faulty nodes are kept on a network, they can cause damage.

16.   Claims 19 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to

Radia et al. as applied to claims 11 and 25 above and further in view of U.S. Patent No.

6,301,668 to Gleichauf et al.

Shipley and Radia do not discuss the management of the various nodes.

Gleichauf discloses a system for maintaining a network map having real-time

information for all nodes in a network for assessing network vulnerabilities (see column

7, lines 26-60), and further notes that can more reliably detect policy violations and

patterns of misuse (see column 3, lines 7-13).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shipley and Radia by maintaining

a network map, as disclosed by Gleichauf, in order to more reliably detect policy

violations and patterns of misuse.

17.   Claim 20 and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 6,295,276 to

Datta et al.

As per claims 20 and 22, Shipley discloses a system for wherein several

methods are disclosed for detecting abnormal usage characteristics (see column 5, line

58 to column 6, line 67). The system user-transparently then reacts by blocking all

access to the LAN from a sender which is associated with a security breach (see

column 8, lines 4-9 and column 10, lines 25-27). A signal is transmitted from the INSD

to the firewall via a serial connection or LAN connection; they therefore constitute

separate nodes. The detecting step is performed at the INSD, while the corrective steps

are performed at other nodes, such as the firewall (see column 5, lines 1-43).

Shipley does not disclose routing via redundant links.

Datta discloses the use of redundant routers for network access, as it provides

better fault tolerance and higher speed connections to a LAN (see abstract).

Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made to modify the network disclosed by Shipley to have redundant

connections at access points, as it provides better fault tolerance and higher speed

connections to a LAN.

Since Shipley's invention demands that a user be denied all access to a network,

one skilled in the art would design the invention to disallow network access on all

redundant routers in the modified configuration.

As per claim 23, the process is inherently performed in real-time.

Regarding claim 24, all modern network implementations having at least the

number of nodes as depicted in Figure 1 are inherently capable of supporting at least

two sessions (secure or otherwise) between at least two pairs of nodes. The invention

of Shipley disallows network access to users attempting a security breach (see column

8, lines 8-17); this can only be done at the point where the user enters the network

(such as the router 22 in Figure 1).

18.   Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et

al. as applied to claim 30 above, and further in of U.S. Patent No. 5,606,668 to Shwed.

Shipley and Radia do not disclose a human interface for supervising the system.

Shwed discloses a system administrator (which is inherently an authenticated

user in a secure network) workstation on the network (see column 4, lines 27-42), and

suggests that the invention is user by the system administrator to change the filtering or

write code (see column 2, lines 5-8).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shipley and Radia by having a

system administrator workstation, as disclosed by Shwed, so the system administrator

can change the filtering or write code.

Allowable Subject Matter

19.   Claims 29 and 35-48 are allowed for the reasons stated in the previous office

action.

Response to Arguments

20.   Applicant's arguments regarding claims 11 and 25 filed 27 February 2006 have

been fully considered but they are not persuasive.

    . Regarding Applicant's arguments regarding claim 11, the amendment does not

affect the meaning of the claim as it was previously construed and is therefore not

sufficient to overcome the previously stated rejection.

    Regarding Applicant's arguments that the rejection of claim 25 (see Remarks, p.

15) does not teach to the use of at least two locking routers, it is noted that the primary

reference, Shipley, suggest the use of two or more routers and that the secondary

reference, Radia, suggests the use locking routers in a manner that would motivate one

skilled in the art to modify Shipley's invention. The claimed invention is therefore

rendered obvious.

    Applicant's arguments, see Remarks, filed 27 February 2006, with respect to the

rejections of all other claims under 35 U.S.C. 102 and 35 U.S.C. 103 have been fully

considered and are persuasive in view of Applicant's amendments. Therefore, the

rejections have been withdrawn. However, upon further consideration, a new ground(s)

of rejection is made in view of the art cited above.

Conclusion

21.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

22.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Matthew E. Heneghan, whose telephone number is

(571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30

AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Jacques Louis-Jacques, can be reached at (571) 272-6962.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is (571) 272-

2100.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

MEH /q/

April 24, 2006